DISCO™

State of ~~Love &~~ Trust

Sean Frazier Advisory CISO - Federal
sean@duo.com | @seanfsez

PEARL JAM
STATE OF LOVE AND TRUST
RADIO PROMO CD – TAKEN FROM THE 'SINGLES' O.S.T.
1. STATE OF LOVE AND TRUST
Promotion Only - Not For Resale

DUO

Duo Security is now part of Cisco. CISCO

ZERO TRUST
I DON'T THIN THIS MEANS WHAT YOU THIN IT MEANS
imgflip.com

ZERO TRUST

130

What is Zero Trust, industry edition?

- 2004ish - Jericho Commandments
- 2010 - John Kindervag, father of Zero Trust
- 2014 - Google BeyondCorp
- 2017 - O’reilly Zero Trust Networks

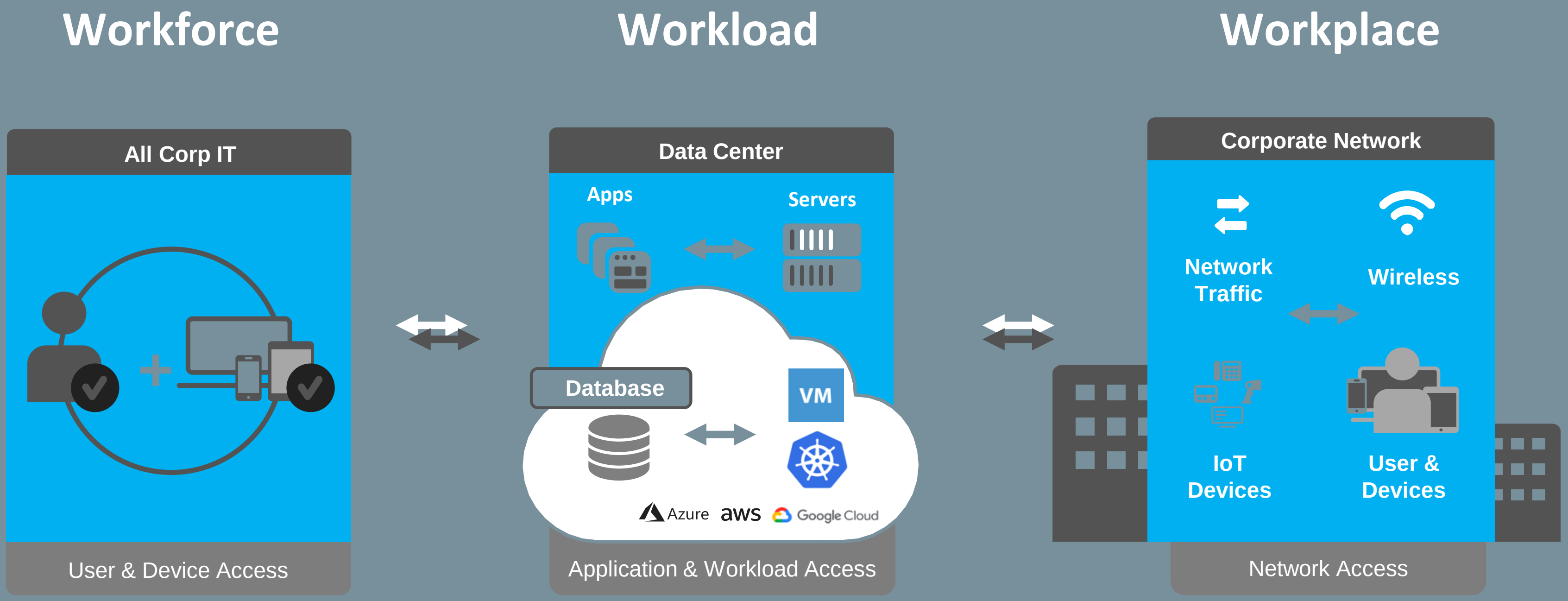
amazon
web services™

Perimeter?

11:42
7
Mail
Wednesday
25
Calendar
Photos
Camera
280
Maps
Clock
Weather
Stocks
Wallet
Notes
Reminders
News
iTunes Store
App Store
iBooks
Home
Health
Settings
DUO
Duo Mobile
Salesforce
Phone
Safari
Messages
Music

Securing Access in the Enterprise

Access happens everywhere – how do establish trusted access?



Workforce

All Corp IT

User & Device Access

Workload

Data Center

Apps

Servers

Database

VM

Azure aws Google Cloud

Application & Workload Access

Workplace

Corporate Network

Network Traffic

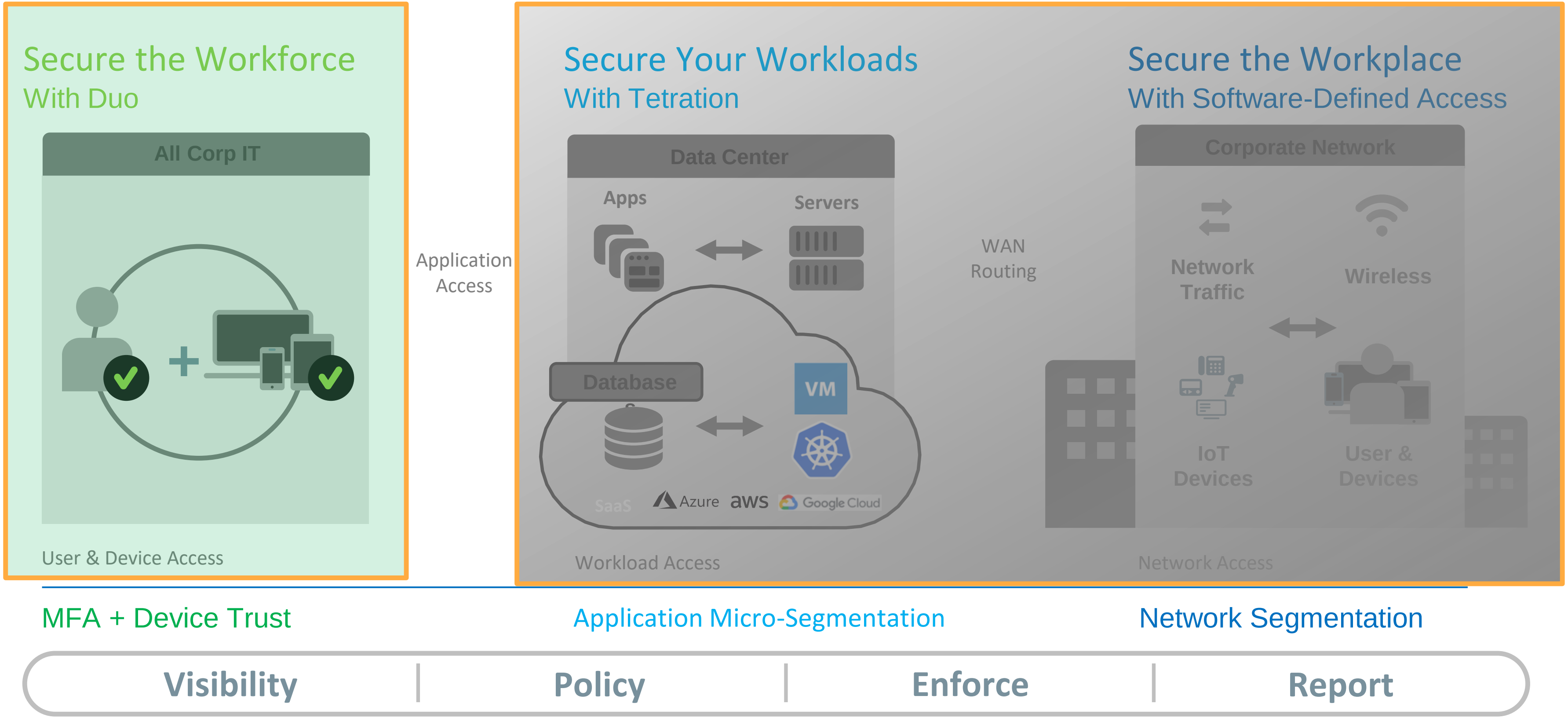
Wireless

IoT Devices

User & Devices

Network Access

Cisco Zero Trust



Secure the Workforce
With Duo

All Corp IT

User & Device Access

Application Access

Secure Your Workloads
With Tetration

Data Center

Apps

Servers

Database

Workload Access

WAN Routing

Secure the Workplace
With Software-Defined Access

Corporate Network

Network Traffic

Wireless

IoT Devices

User & Devices

Network Access

MFA + Device Trust

Application Micro-Segmentation

Network Segmentation

Visibility | Policy | Enforce | Report

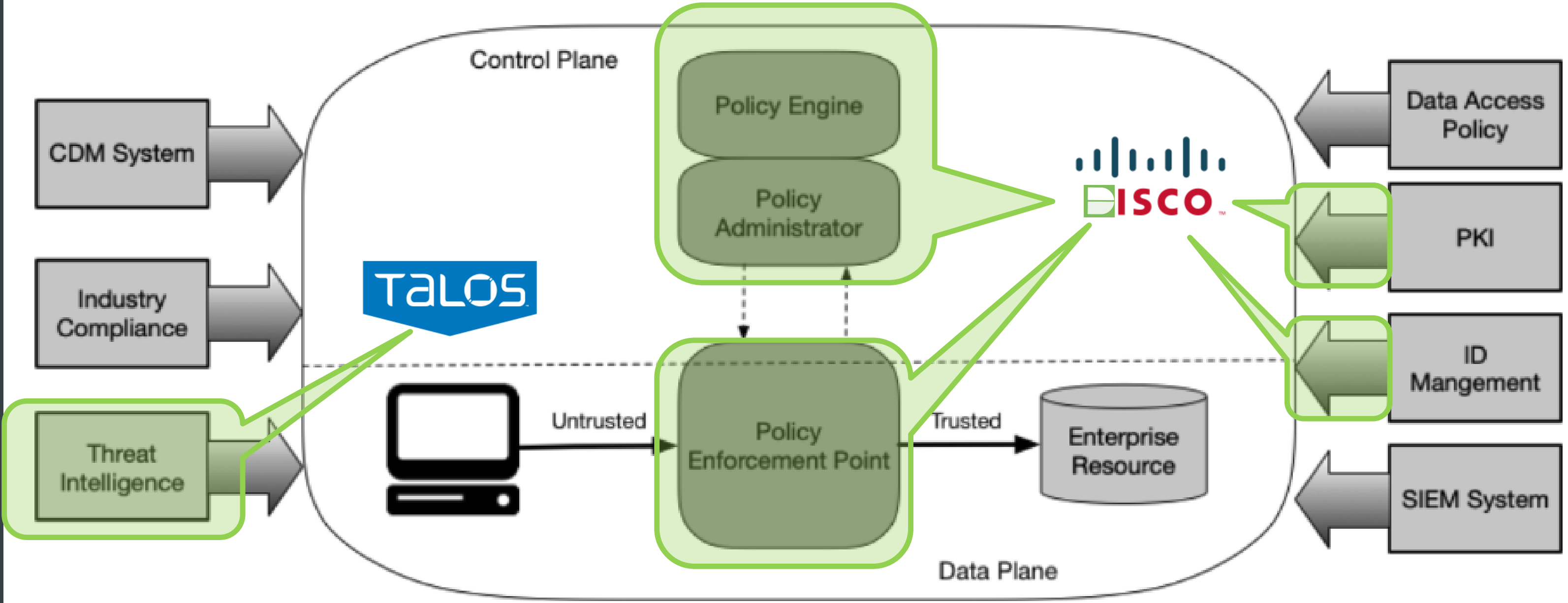
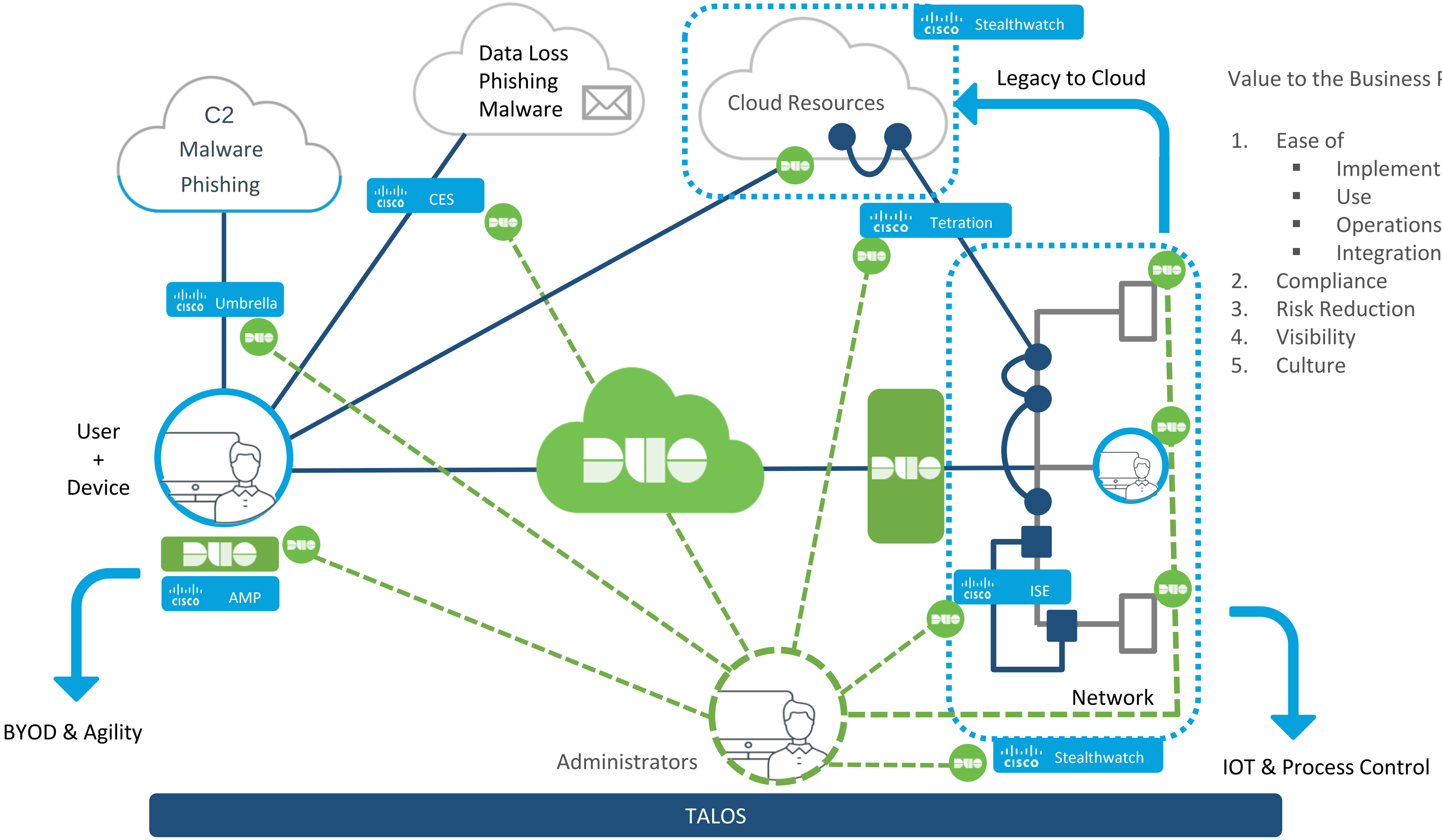


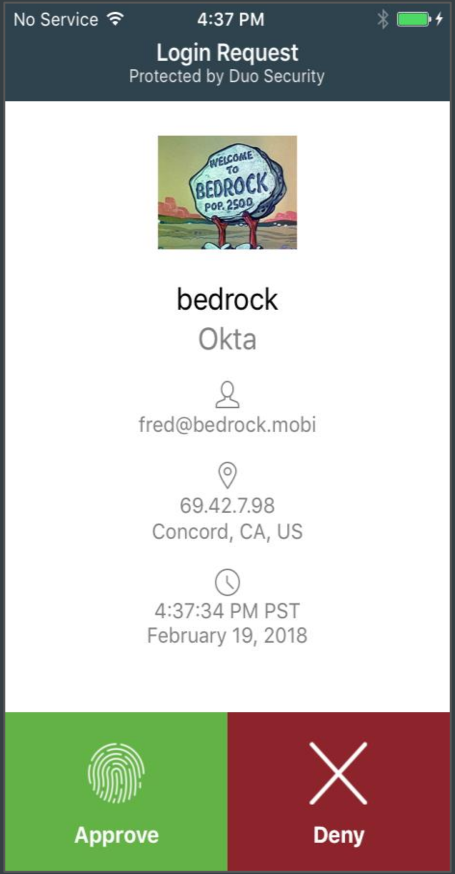
Figure 2: Core Zero Trust Logical Components

The User Journey – Cisco Zero Trust



Value to the Business Priorities

1. Ease of
   - Implementation
   - Use
   - Operations/FTE
   - Integration
2. Compliance
3. Risk Reduction
4. Visibility
5. Culture



No Service 4:37 PM

Login Request

Protected by Duo Security

bedrock

Okta

fred@bedrock.mobi

69.42.7.98

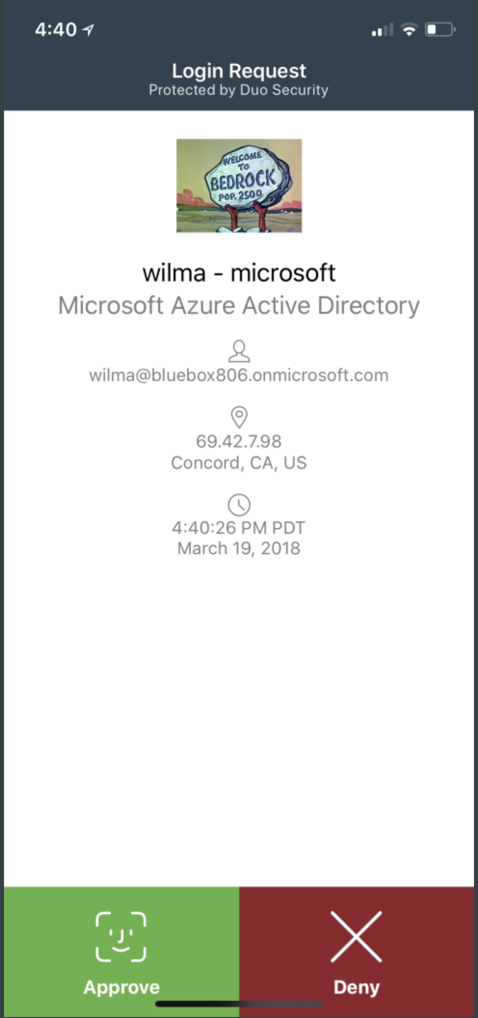
Concord, CA, US

4:37:34 PM PST

February 19, 2018

Approve

Deny



4:40

Login Request

Protected by Duo Security

wilma - microsoft

Microsoft Azure Active Directory

wilma@bluebox806.onmicrosoft.com

69.42.7.98

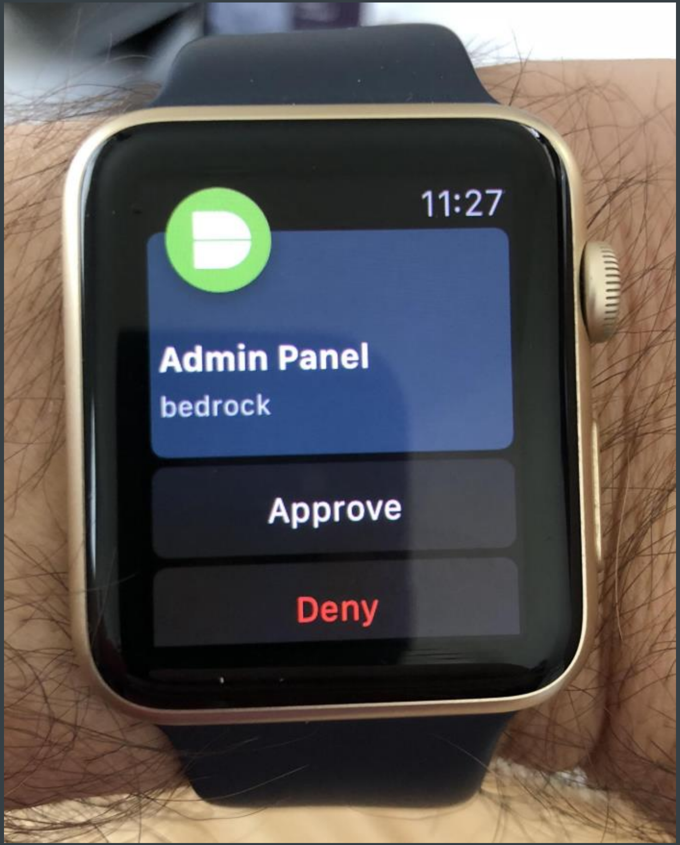
Concord, CA, US

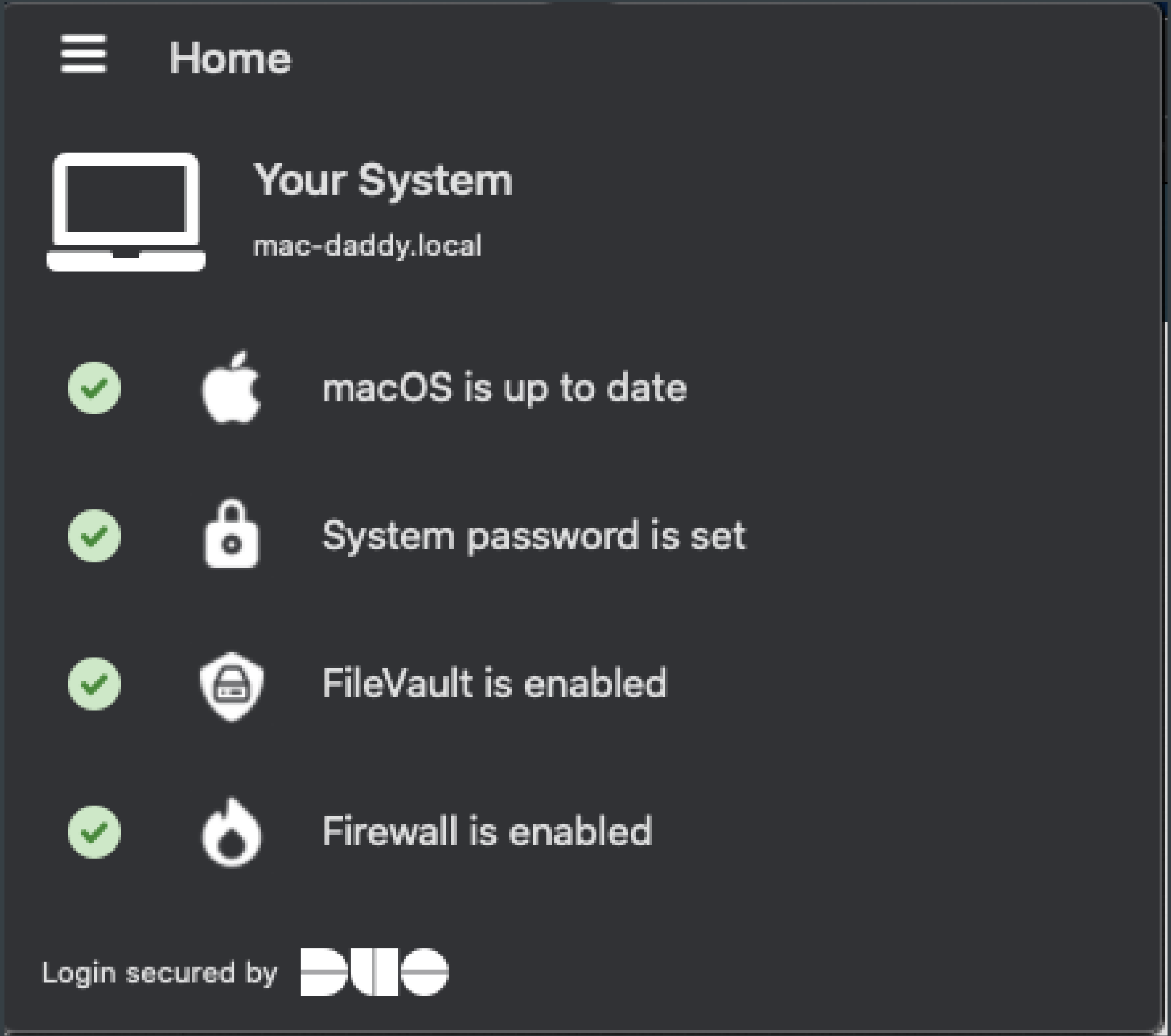
4:40:26 PM PDT

March 19, 2018

Approve

Deny





Home

Your System

mac-daddy.local

✓ macOS is up to date

✓ System password is set

✓ FileVault is enabled

✓ Firewall is enabled

Login secured by DUO

Wired for Zero Trust

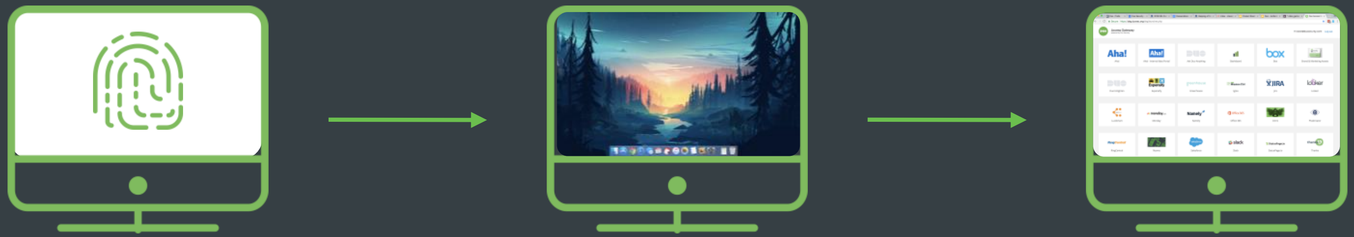
Integration documents are available at **duo.com/docs**

Microsoft	VPNs	Cloud Apps	On-Premises	Identity	Custom
Office 365	JUNIPER NETWORKS	salesforce	Epic	Microsoft Active Directory	REST APIS
Outlook	CISCO	Google Apps	ORACLE PEOPLESOFT	Active Directory Federation Services	WEB SDK
Remote Desktop Services	CiTRIX	amazon web services	vmware Horizon View	okta	RADIUS
Windows Server	paloalto NETWORKS	box	>_SSH unix	PingIdentity	SAML
RRAS	Pulse Secure	Dropbox	Shibboleth	onelogin	OIDC

STEVEN SPIELBERG PRESENTS
BACK TO THE FUTURE
PG
A ROBERT ZEMECKIS FILM
OUTATIME

Our Vision: Passwordless Authentication

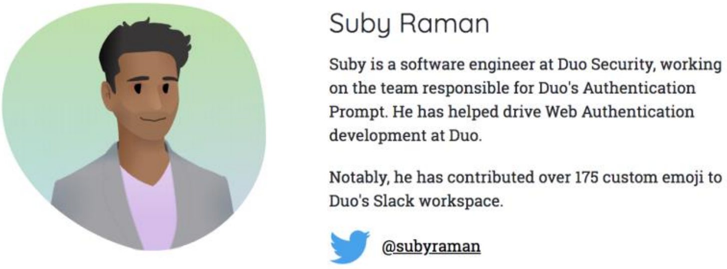
User to Device → To Every Application



webauthn.guide / webauthn.io

WebAuthn

A better alternative for securing
our sensitive information online



Suby Raman

Suby is a software engineer at Duo Security, working on the team responsible for Duo's Authentication Prompt. He has helped drive Web Authentication development at Duo.

Notably, he has contributed over 175 custom emoji to Duo's Slack workspace.

@subyraman

fido™

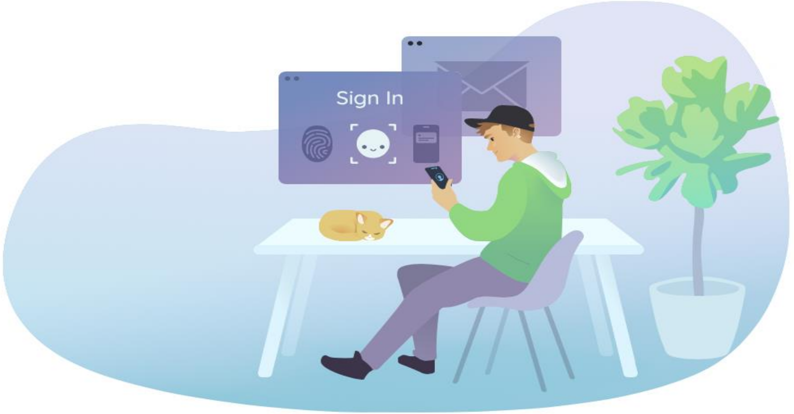
W3C

Nick Steele

Nick Steele is an R&D engineer with Duo Labs and a W3C Invited Expert for the WebAuthn standard.

While his focus lies in user authentication and authorization, he also has strong opinions about sci-fi and ramen.

@codekaiju



DUO Duo Security is now part of Cisco. CISCO

Trust Engine

https://duo.com/labs

https://twitter.com/duo_labs

DISCO
TM

What is BeyondCorp?

- 2014 - Google BeyondCorp paper
- 2016 - Google BeyondCorp progress update
- 2017 - BeyondCorp migration, user experience and lessons learned

SECURITY

BeyondCorp
A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

Rory Ward is a site reliability engineering manager in Google Ireland. He previously worked in Ireland at Valista, in Silicon Valley at AOL, Netscape, Kiva, and General Magic, and in Los Angeles at Retix. He has a BSc in computer applications from Dublin City University. roryward@google.com

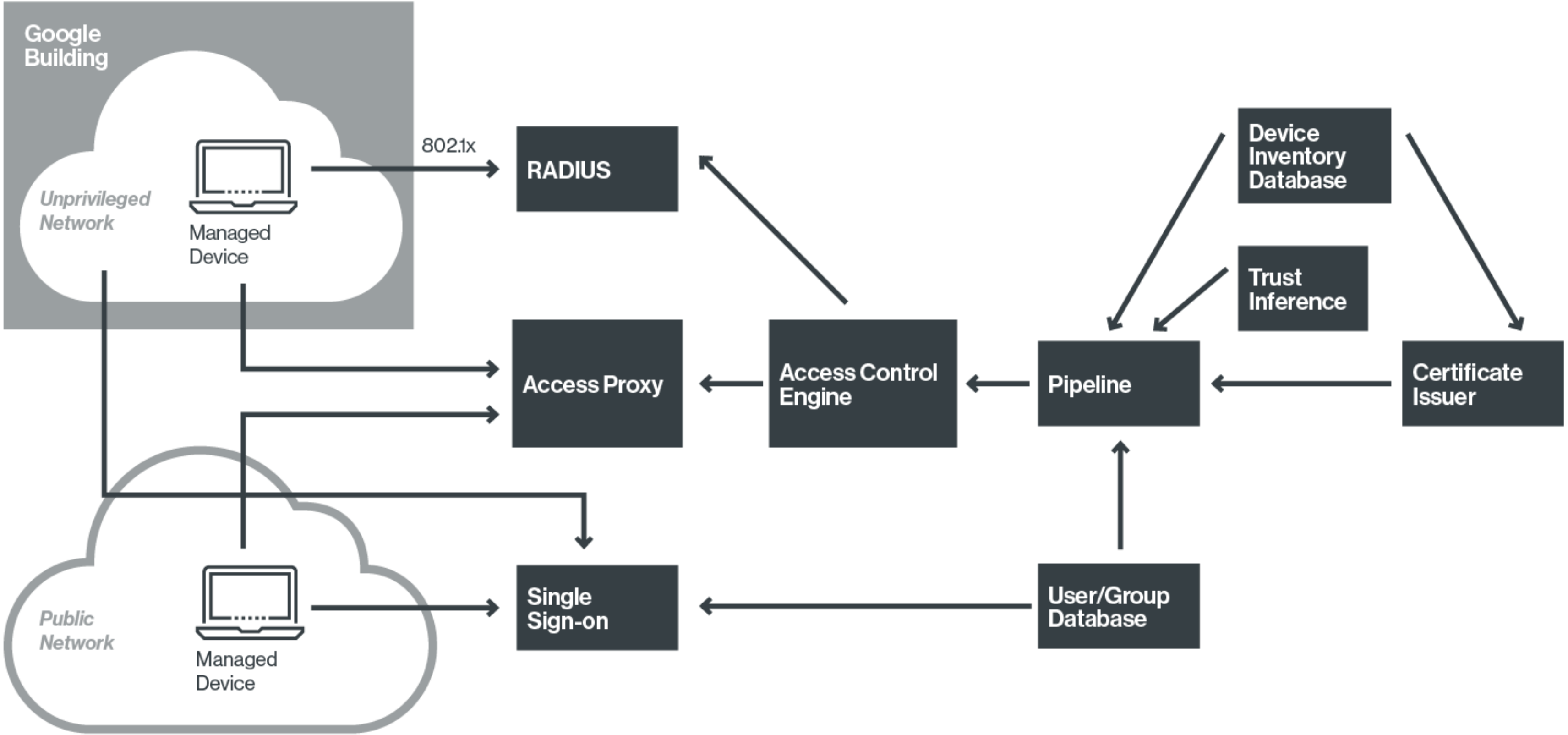
Betsy Beyer is a technical writer specializing in virtualization software for Google SRE in NYC. She has previously provided documentation for Google Data Center and Hardware Operations teams. Before moving to New York, Betsy was a lecturer in technical writing at Stanford University. She holds degrees from Stanford and Tulane. bbeyer@google.com

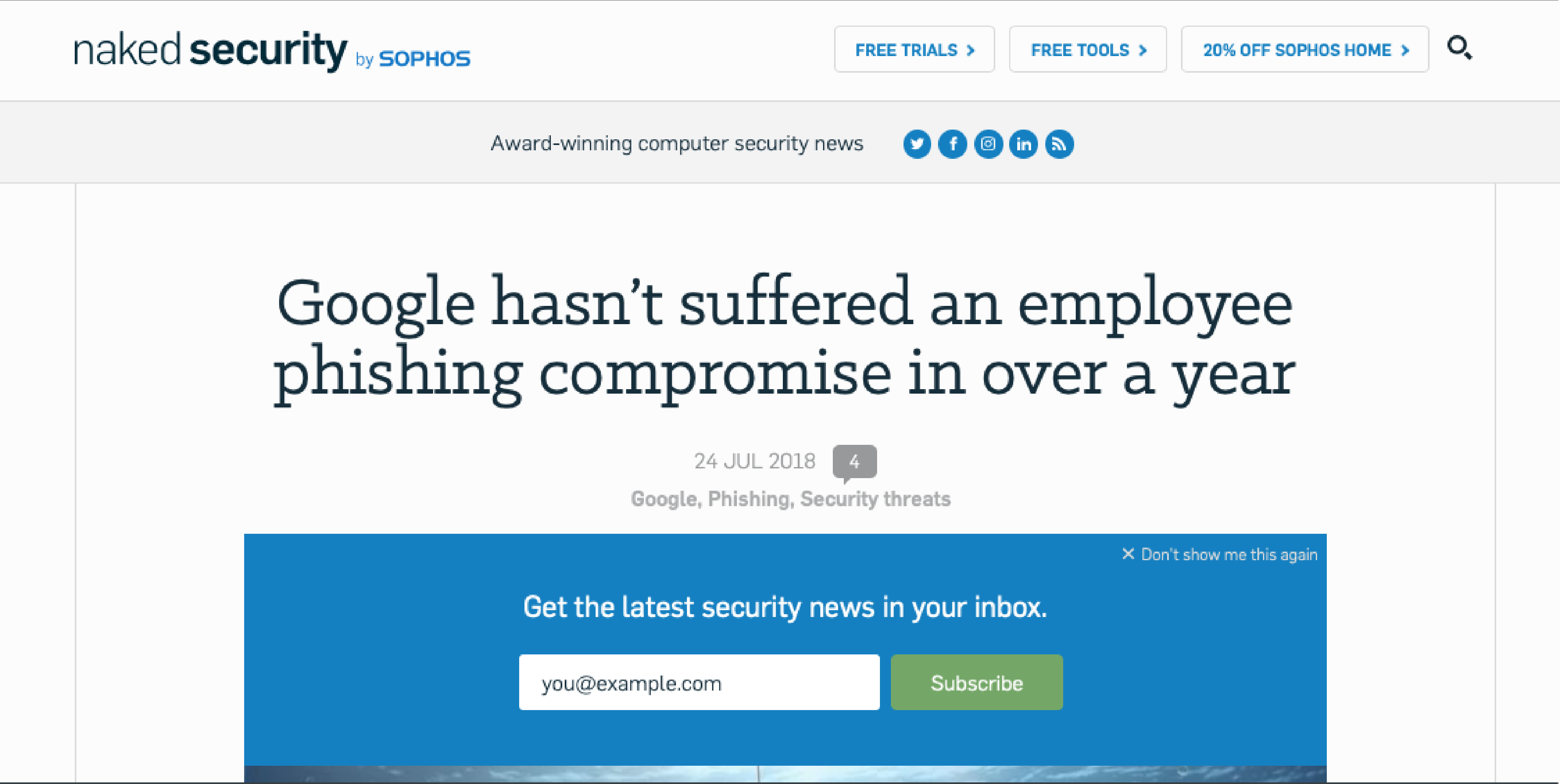
Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company's privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gate access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit. Anything located outside the wall is considered dangerous, while anything located inside the wall is trusted. Anyone who makes it past the drawbridge has ready access to the resources of the castle.

The perimeter security model works well enough when all employees work exclusively in buildings owned by an enterprise. However, with the advent of a mobile workforce, the surge in the variety of devices used by this workforce, and the growing use of cloud-based services, additional attack vectors have emerged that are stretching the traditional paradigm to the point of redundancy. Key assumptions of this model no longer hold: The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications.

Google BeyondCorp: Zero-Trust at Work





Google hasn't suffered an employee phishing compromise in over a year

24 JUL 2018 4

Google, Phishing, Security threats

Get the latest security news in your inbox.